#2

Rec'd PCT/PTO 14 OCT 2004

PATENTTI- JA REKISTERIHALLI[redacted]
NATIONAL BOARD OF PATENTS A[redacted]REGISTRATION

PC[redacted]02/01033

Helsinki 29.1.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

REC'D 12 FEB 2003
WIPO PCT

Hakija
Applicant

Nokia Corporation
Helsinki

Patenttihakemus nro
Patent application no

20020733

Tekemispäivä
Filing date

16.04.2002

Kansainvälinen luokka
International class

H04L

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestelmä tiedonsiirtolaitteen käyttäjän autentikointiin"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Kristina Laukkasuo
Tarkastaja

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A
P.O.Box 1160
FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Menetelmä ja järjestelmä tiedonsiirtolaitteen käyttäjän autentikointiin

Ala

Keksinnön kohteina ovat menetelmä tiedonsiirtolaitteen käyttäjän autentikointiin ja järjestelmä tiedonsiirtolaitteen käyttäjän autentikointiin.

Tausta

Tiedonsiirtolaitteen käyttäjän autentikointiin tunnetaan erilaisia menetelmiä. Eräs autentikointimenetelmä perustuu tiedonsiirtolaitteeseen sijoitetun SIM-kortin (Subscriber Identity Module) käyttöön, tällöin kuitenkin tiedonsiirtolaitteessa täytyy olla älykortin lukija. Ratkaisua ei myöskään ole helppo soveltaa tilanteissa, joissa halutaan tilapäisesti, ehkä jopa vain yhden kerran, käyttää tiedonsiirtolaitteella jotakin tiedonsiirtopalvelua, sillä sehän edellyttää SIM-kortin toimittamista käyttäjän tiedonsiirtolaitteeseen.

Tähän viitteeksi otettavassa US-patentissa 6,112,078 kuvataan ilman SIM-korttia toimiva ratkaisu, jossa ainakin osa autentikointidatasta lähetetään tiedonsiirtolaitteen käyttäjän hallussa olevaan matkapuhelimeen tai hakulaitteeseen. Ratkaisussa kaikkea autentikointidataa, esimerkiksi käyttäjätunnusta ja salasanaa, ei lähetetä samaa siirtotietä pitkin tietoturvasyistä.

Lyhyt selostus

Keksinnön tavoitteena on tarjota parannettu menetelmä tiedonsiirtolaitteen käyttäjän autentikointiin ja parannettu järjestelmä tiedonsiirtolaitteen käyttäjän autentikointiin.

Keksinnön eräänä puolena esitetään menetelmä tiedonsiirtolaitteen käyttäjän autentikointiin, joka menetelmä käsittää: muodostetaan tiedonsiirtolaitteella tiedonsiirtoyhteys palvelupisteeseen; syötetään palvelupisteeseen matkaviestinjärjestelmän tilaajan tunnistetieto; tarkistetaan matkaviestinjärjestelmästä matkaviestinjärjestelmän tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen; ja jos käyttöoikeus on voimassa, generoidaan salasana, lähetetään salasana matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen, ja sisäänkirjaudutaan tiedonsiirtolaitteella palvelupisteeseen käyttäen salasanana tilaajapäätelaitteeseen toimitettua salasanaa.

Keksinnön eräänä puolena esitetään järjestelmä tiedonsiirtolaitteen käyttäjän autentikointiin, joka järjestelmä käsittää tiedonsiirtolaitteen, tiedonsiirtolaitteeseen ensimmäisellä tiedonsiirtoyhteydellä kytkettävissä olevan palve-

lupisteen, ja palvelupisteeseen toisen tiedonsiirtoyhteyden välityksellä kytketyn autentikointipalvelimen; ja palvelupiste on konfiguroitu vastaanottamaan ensimmäistä tiedonsiirtoyhteyttä pitkin tiedonsiirtolaitteella syötetty matkaviestinjärjestelmän tilaajan tunnistetieto, ja lähettämään matkaviestinjärjestelmän tilaajan tunnistetieto toista tiedonsiirtoyhteyttä pitkin autentikointipalvelimelle; autentikointipalvelin on konfiguroitu tarkistamaan kolmatta tiedonsiirtoyhteyttä käyttäen matkaviestinjärjestelmästä matkaviestinjärjestelmän tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen, ja jos käyttöoikeus on voimassa, generoimaan salasana ja lähettämään salasana matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen; ja tiedonsiirtolaite on konfiguroitu palvelupisteeseen sisäänkirjauduttaessa käyttämään salasanana tilaajapäätelaitteeseen toimitettua salasanaa.

Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että tiedonsiirtolaitteen käyttäjän autentikoinnissa hyödynnetään matkaviestinjärjestelmän tilaajan tunnistetietoa. Ainakin salasana lähetetään matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen. Kyseiselle matkaviestinjärjestelmän tilaajan tunnistetiedolle on merkitty käyttöoikeus haluttuun palvelupisteeseen.

Keksinnön mukaisella menetelmällä ja järjestelmällä saavutetaan useita etuja. Tiedonsiirtolaitteen käyttäjän autentikointi ei edellytä ylimääräistä laitteiston tai ohjelmiston käyttöä tiedonsiirtolaitteessa, ainoastaan matkaviestinjärjestelmän tilaajapäätelaitteen omistamista tai lainaamista. Ratkaisu toimii myös tilaajapäätelaitteen verkkovierailun (Roaming) aikana. Ratkaisu on myös helppo palvelupistettä hallinnoivalle operaattorille, käyttöoikeuden antaminen (Provisioning) ei edellytä esimerkiksi SIM-kortin toimittamista käyttäjälle, mutta kuitenkin autentikointi tavallaan perustuu olemassaolevaan, tilaajapäätelaitteeseen sijoitettuun SIM-korttiin.

Kuvioluettelo

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joissa

kuvio 1 on yksinkertaistettu lohkokaavio havainnollistaen järjestelmää tiedonsiirtolaitteen käyttäjän autentikointiin;

kuvio 2 on vuokaavio havainnollistaen menetelmää tiedonsiirtolaitteen käyttäjän autentikointiin; ja

kuvio 3 on signaalisekvenssikaavio kuvaten tiedonsiirtolaitteen käyttäjän autentikoinnissa eri verkkoelementtien välillä lähetettävää informaatiota.

Suoritusmuotojen kuvaus

Kuviossa 1 kuvataan yksinkertaistettu esimerkki järjestelmästä tiedonsiirtolaitteen 100 käyttäjän autentikointiin, lisäksi on kuvattu järjestelmän yhteydet muihin tarvittaviin osiin, joiden kanssa vaihdetaan informaatiota, ja joita käytetään tiedonsiirtoyhteyksien toteuttamiseen.

Osat voidaan jakaa neljään pääosaan: käyttäjän hallussa olevat laitteet 104, tiedonsiirtolaitetta 100 palveleva tiedonsiirtoverkko 118, vierailtava matkaviestinjärjestelmä 126, ja kotimatkaviestinjärjestelmä 134.

Tiedonsiirtoverkko 118 käsittää tiedonsiirtolaitteeseen 100 ensimmäisellä tiedonsiirtoyhteydellä 102 kytkettävissä olevan palvelupisteen (Service Access Point, SAP) 110. Palvelupiste 110 muodostaa ns. pääsyvyöhykkeen (Access Zone, AZ, tunnetaan myös nimellä Hotspot), esimerkiksi toimistossa, yliopiston kampusalueella, hotellissa tai lentokentällä, jossa lähiverkkoyhteyksiä tarjotaan käyttäjille. Esimerkiksi kannettavan tietokoneen käyttäjille voidaan siten tarjota nopea langaton laajakaistainen palvelu pääsyvyöhykkeen välityksellä. Lisäksi tiedonsiirtoverkko 118 käsittää palvelupisteeseen 110 toisen tiedonsiirtoyhteyden välityksellä kytketyn autentikointipalvelimen 114.

Eräässä suoritusmuodossa ensimmäinen tiedonsiirtoyhteys 106 on radioyhteys. Radioyhteys 106 voidaan toteuttaa siten, että palvelupiste 110 on konfiguroitu toteuttamaan radioyhteys 106 langattomalla lähiverkolla (WLAN, Wireless Local Area Network). Eräässä suoritusmuodossa palvelupiste 110 käsittää lyhyen kantaman radiolähetinvastaanottimen radioyhteyden 106 toteuttamiseksi. Lyhyen kantaman radiolähetinvastaanotin voi olla esimerkiksi Bluetooth®-teknologian mukainen radiolähetinvastaanotin, tai IEEE:n (The Institute of Electrical and Electronics Engineers, Inc.) standardin 802.11 tai 802.11b mukainen langaton lähiverkko.

Palvelupisteen 110 tehtävänä on toimia porttina, jonka kautta tiedonsiirtoverkon 118 palvelut tarjotaan tiedonsiirtolaitteelle 100. Jos ensimmäinen tiedonsiirtoyhteys 106 toteutetaan langattomalla lähiverkolla, palvelupisteenä 110 voidaan käyttää langattoman lähiverkon palvelupistettä, esimerkiksi Nokia® A032-tyyppistä langattoman lähiverkon palvelupistettä, joka toimii langattomana Ethernet-siltana lähiverkkoon. Palvelupiste 110 käsittää tällöin radiomodulin radioyhteyksien toteuttamiseksi, ja radioyhteyksien tiedon salaukseen (Encryption) tarvittavat laitteistot ja ohjelmistot. Palvelupiste 110 voi myös

sisältää ulkoisen modeemin, jolla voidaan toteuttaa soittoyhteys (Dial-up Access) Internet-palvelun tarjoajaan (Internet Service Provider, ISP), jolloin palvelupiste 110 voi sisältää paikallisverkon suojelemiseksi palomuurin, esimerkiksi NAT-teknologialla (Network Address Translation) toteutetun palomuurin.

Tiedonsiirtoverkko 118 voi käsittää myös palvelupisteen 110 ja autentikointipalvelimen 114 välissä pääsykontrollerin (Access Controller, AC) 112, joka toimii yhdyskäytävänä pääsyvyöhykkeen ja Internetin välillä. Tiedonsiirtoverkosta 118 voidaan siis pääsykontrollerin 112 välityksellä päästä myös johonkin WWW-palvelimeen (World-Wide Web), jonka kanssa tiedonsiirtolaite 100 voi autentikoinnin jälkeen vaihtaa informaatiota. Pääsykontrollerina 112 voidaan käyttää esimerkiksi Nokia® P022-tyyppistä pääsykontrolleria, joka vastaa käyttäjien autentikoinnista, monitoroi verkon käyttöä reaaliajassa ja kerää laskentatietoa laskutusta varten.

Eräässä suoritusmuodossa autentikointipalvelin 114 on AAA-palvelin (Authentication, Authorization, and Accounting), jolloin käyttäjän todentamisen (Authentication), eli käyttäjän väitetyn identiteetin vahvistamisen lisäksi se huolehtii käyttövaltuuksien myöntämisestä (Authorization) järjestelmään, ja laskennasta (Accounting) järjestelmän käytön laskuttamiseksi. Autentikointipalvelin 114 voi tällöin käyttää IETF:n (Internet Engineering Task Force) määrittelemää AAA-protokollaa, esimerkiksi Radius-protokollaa (Remote Authentication Dial-in User Service, RADIUS) tai Diameter-protokollaa. Langattomassa lähiverkossa autentikointipalvelin 114 siirtää autentikointidataa ja laskutustietoa tiedonsiirtoverkon 118 ja matkaviestinjärjestelmän 126, 134 välillä.

Eräässä suoritusmuodossa ensimmäinen tiedonsiirtoyhteys 106 on langallinen. Tiedonsiirtoyhteys voidaan toteuttaa tällöin millä tahansa tunnetulle verkkoteknologialla, joka mahdollistaa kaksisuuntaisen langallisen tiedonsiirtosiirron palvelupisteen 110 ja tiedonsiirtolaitteen 100 välillä. Esimerkkinä tällaisesta verkkoteknologiasta voidaan mainita IEEE:n 802.3 standardin, eli Ethernet-standardin, mukainen langallinen lähiverkko, jossa langallisuus toteutetaan esimerkiksi koaksiaalikaapelia tai kierrettyä paria käyttäen.

Kuviossa 1 on siis kuvattu eräitä osia vierailtavasta matkaviestinjärjestelmästä 126 ja kotimatkaviestinjärjestelmästä 134, sillä eräässä suoritusmuodossa ensimmäinen tiedonsiirtoyhteys 106 muodostetaan tilaajapäätelaitteen 102 verkkovierailun aikana. Verkkovierailutoiminto on funktionaalinen entiteetti liikkuvuuden hallinnassa (Mobility Management, MM), joka mahdollistaa oikean puhelun väylöityksen (Routing) käyttäjän liikkuessa tilaajapäätelaittei-

neen 102 verkosta toiseen, esimerkiksi kotimaassaan olevasta kotimaisen operaattorin hallinnoimasta matkaviestinjärjestelmästä 134 ulkomailla olevaan ulkomaisen operaattorin hallinnoimaan matkaviestinjärjestelmään 126. Myös sellainen suoritusmuoto on mahdollinen, jossa tarvitaan vain kotimatkaviestinjärjestelmä 134, esimerkiksi käyttäjän pysytellessä kotimaassaan. Tällöin jatkossa esitettävän selostuksen kannalta kuviossa 1 esitettävien matkaviestinjärjestelmien 126, 134 osat ovat soveltuvin osin samassa matkaviestinjärjestelmässä.

Matkaviestinjärjestelmä 126, 134 voi olla mikä tahansa tunnettu radiojärjestelmä, jossa on mahdollista siirtää informaatiota matkaviestinjärjestelmän verkko-osasta siihen radioyhteydellä 108 kytkettyyn tilaajapäätelaitteeseen 104. Esimerkkeinä matkaviestinjärjestelmistä voidaan mainita toisen sukupolven GSM (Global System for Mobile Communications), 2,5:n sukupolven EDGE-tekniikkaa (Enhanced Data Rates for Global Evolution) tiedonsiirtonopeuden kasvattamiseksi käyttävä GSM:ään perustuva GPRS-järjestelmä (General Packet Radio System) tai EGPRS-järjestelmä (Enhanced GPRS), ja kolmannen sukupolven matkaviestinjärjestelmä, joka tunnetaan ainakin nimillä IMT-2000 (International Mobile Telecommunications 2000) ja UMTS (Universal Mobile Telecommunications System). Suoritusmuodot eivät kuitenkaan rajaudu vain näihin esimerkkeinä mainittuihin järjestelmiin, vaan alan ammattilainen voi soveltaa opetuksia myös muissa vastaavat ominaisuudet sisältävissä radiojärjestelmissä. Matkaviestinjärjestelmästä on tarvittaessa saatavissa lisätietoja spesifikaatioista, esimerkiksi GSM-järjestelmän tai UMTS-järjestelmän spesifikaatioista, ja alan kirjallisuudesta, esimerkiksi teoksesta Juha Korhonen: Introduction to 3G Mobile Communications. Artech House 2001. ISBN 1-58053-287-X.

Palvelupiste 110 on konfiguroitu vastaanottamaan ensimmäistä tiedonsiirtoyhteyttä 106 pitkin tiedonsiirtolaitteella 100 syötetty matkaviestinjärjestelmän tilaajan tunnistetieto, ja lähettämään matkaviestinjärjestelmän tilaajan tunnistetieto toista tiedonsiirtoyhteyttä pitkin autentikointipalvelimelle 114. Eräässä suoritusmuodossa matkaviestinjärjestelmän 134 tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero (Mobile Subscriber International Integrated Services Digital Network Number, MSISDN), joka yksilöi tilaajan maailmanlaajuisesti yksikäsitteisesti, sillä MSISDN muodostuu kolmesta osasta: maatunnus, kansallinen verkkotunnus, ja tilaajanumero.

Autentikointipalvelin 114 on konfiguroitu tarkistamaan kolmatta tiedonsiirtoyhteyttä käyttäen matkaviestinjärjestelmästä 134 tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen 110, ja jos käyttöoikeus on voimassa, generoimaan salasana ja lähettämään salasana matkaviestinjärjestelmän 134 tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen 102. Autentikointipalvelin 114 voi myös generoida tarvittavan käyttäjätilin (User Account), ellei sitä jo ole ennestään olemassa. Tiedonsiirtolaite 100 on konfiguroitu palvelupisteeseen 110 sisäänkirjauduttaessa (Login) käyttämään salasanana tilaajapäätelaitteeseen 102 toimitettua salasanaa. Generoitu salasana voi olla merkkijono (Character String), joka sisältää esimerkiksi aakkosia ja/tai numeroita ja/tai erilaisia erikoismerkkejä. Merkkijono voidaan määritellä esimerkiksi ASCII-koodeja (American Standard Code for Information Intrerchange) käyttäen. Sisäänkirjautuminen voidaan suorittaa esimerkiksi WWW-dialogia tai IEEE:n 802.1x-standardin mukaisesti tiedonsiirtolaitteen käyttöjärjestelmän dialin-dialogia käyttäen.

Tiedonsiirtolaite 100 on sellainen, että se kykenee muodostamaan kaksisuuntaisen tiedonsiirtoyhteyden 106 palvelupisteeseen 110. Tiedonsiirtolaite voi siten olla esimerkiksi kännettava tietokone, joka on varustettu Ethernet-kortilla, Bluetooth®-lähetinvastaanottimella, tai langattoman lähiverkon toteuttavalla kortilla, jossa on radiolähetinvastaanotin, esimerkiksi lyhyenkantaman radiolähetinvastaanotin. Eräs esimerkki lähiverkon toteuttavasta kortista on Nokia® C110/C111-tyyppinen langaton lähiverkkokortti, kuitenkin on huomattava, että järjestelmä käyttäjän autentikointiin toimii ilman kyseisissä korteissa olevaa SIM-kortin lukijaa. Toinen esimerkki on Nokia® D211-tyyppinen radiokortti, joka toimii useissa eri moodeissa tiedonsiirtoyhteyden toteuttamiseksi: langaton lähiverkko, GPRS, ja HSCSD (High Speed Circuit Switched Data).

Tilaajapäätelaite 102 on sellainen, että sillä voidaan toteuttaa langaton tiedonsiirtoyhteys matkaviestinjärjestelmään 126. Esimerkiksi UMTS-järjestelmän tilaajapäätelaite 102 koostuu kahdesta osasta: matkaviestinlaite (Mobile Equipment, ME) ja UMTS-tilaajan tunnistusyksikkö (UMTS Subscriber Identity Module, USIM) eli SIM-kortti. SIM-kortti sisältää käyttäjään liittyvää tietoa, sekä erityisesti tietoturvallisuuteen liittyvää tietoa, esimerkiksi salausalgoritmin. GSM-järjestelmän tilaajapäätelaite 102 käyttää luonnollisesti GSM-järjestelmän omaa SIM-korttia. Tilaajapäätelaite 102 sisältää ainakin yhden lähetinvastaanottimen, jolla toteutetaan radioyhteys 102 matkaviestinjärjestel-

män 126 radioliityntäverkkoon tai tukiasemajärjestelmään. Kuviossa 1 on kuvattu matkaviestinjärjestelmän 126 tukiasema 120, johon tilaajapäätelaite 102 muodostaa radioyhteyden 108. Yksi tilaajapäätelaite 102 voi sisältää ainakin kaksi erilaista tilaajan tunnistusyksikköä. Lisäksi tilaajapäätelaite 102 sisältää antennin, käyttöliittymän, sekä akun. Nykyisin tilaajapäätelaitteita 102 on monenlaisia, esimerkiksi autoon asennettuja sekä kannettavia. Tilaajapäätelaitteisiin 102 on myös toteutettu ominaisuuksia, jotka ovat paremmin tunnettuja henkilökohtaisista tai kannettavista tietokoneista. Eräs esimerkki tällaisesta tilaajapäätelaitteesta 102 on Nokia® Kommunikaattori®.

Kuvion 1 esimerkissä käyttäjän hallussa olevat laitteet 104, eli tiedonsiirtolaite 100 ja tilaajapäätelaite 102 on kuvattu erillisinä laitteina, mutta eräässä suoritusmuodossa ne voivat sijaita yhdessä fyysisessä laitteessa, esimerkiksi Nokia® Kommunikaattori®-tyyppisessä laitteessa, jossa tiedonsiirtolaitteelta 100 vaadittavat ominaisuudet on toteutettu esimerkiksi langattomalla lähiverkkokortilla ja tilaajapäätelaitteelta 102 vaadittavat ominaisuudet on toteutettu laitteessa olevan matkaviestinjärjestelmän tilaajapäätelaitteella ja matkaviestinjärjestelmän operaattorin antamalla SIM-kortilla. Tällaisessa yhdistetyssä laitteessa voidaan autentikoinnin suorittamiseksi tarvittavien tietojen käsittelyä automatisoida, esimerkiksi siten, että tilaajapäätelaitteeseen 102 vastaanotettu salasana siirretään automaattisesti tiedonsiirtolaitteen 100 sisäänkirjautumisdialogiin.

Eräässä suoritusmuodossa autentikointipalvelin 114 on konfiguroitu lähettämään salasana tilaajapäätelaitteeseen 102 pakettikytkentäisenä viestinä. Eräässä suoritusmuodossa autentikointipalvelin 114 on konfiguroitu lähettämään salasana tilaajapäätelaitteeseen 102 lyhytsanomassa (Short Message, SM). Lyhytsanoma voidaan toteuttaa esimerkiksi tekstiviestipalvelua (Short Message Service, SMS) käyttäen. Kuviossa 1 on kuvattu matkaviestinjärjestelmän 126 lyhytsanomapalvelukeskus (Short Message Service Centre, SMSC) 122, jota kautta lyhytsanomat lähetetään, ja johon ne voidaan tallettaa, ellei niitä saada heti toimitettua vastaanottajalle 102. Periaatetasolla lyhytsanomapalvelukeskus 122 ei kuulu matkaviestinjärjestelmään 126, vaikka se usein integroidaankin matkapuhelinkeskukseen (Mobile Service Switching Center, MSC). Myös muita tapoja tekstin sisältävän viestin lähettämiseen voidaan käyttää, esimerkiksi MMS:ää (Multimedia Messaging Service) käyttäen. MMS on uudenlainen viestipalvelu, joka lähetystavaltaan vastaa SMS-viestiä. MMS-

viesti voi kuitenkin sisältää yhtä aikaa kolme eri elementtiä: tekstin, ääniviestin ja kuvan.

Eräässä suoritusmuodossa autentikointipalvelin 114 on palvelupisteen 110 käyttöoikeuden tarkistamiseksi konfiguroitu lähettämään kysely matkaviestinjärjestelmän 134 kotirekisteriin 130. Kuviossa 1 vierailtavasta matkaviestinjärjestelmästä 126 kuvataan vain tukiasema 120 ja lyhytsanomapalvelukeskus 122; muuta infrastruktuuria kuvataan lohkolla 124. Vierailtavan matkaviestijärjestelmän 126 infrastruktuurista on tiedonsiirtoyhteys, esimerkiksi ITU-T:n, eli Kansainvälisen Televiestintäliiton (International Telecommunication Union, ITU) telestandardointisektorin merkinantojärjestelmä nro 7:ää (SS7, ITU-T No. 7) 128 käyttäen kotimatkaviestinjärjestelmään 134, josta on kuvattu vain kotirekisteri (Home Location Register, HLR) 130, johon kaikkien matkaviestinjärjestelmän 134 tilaajien tilaajaparametrit on pysyvästi tallennettu. Koska kotirekisteri 130 on yleensä matkapuhelinkeskuksen yhteydessä, on kuviossa 1 lohkoon 130 sisällytetty myös matkapuhelinkeskus.

Eräässä aiemmin mainitussa suoritusmuodossa matkaviestinjärjestelmän 134 tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero. Tällöin autentikointipalvelin 114 voidaan konfiguroida kyselyssä ensin selvittämään matkaviestinjärjestelmän 134 kotirekisteristä 130 matkaviestintilaajan kansainvälistä ISDN-numeroa vastaavan kansainvälisen matkaviestintilaajan tunnuksen (International Mobile Subscriber Identity, IMSI), ja sitten selvittämään tilaajatiedot, jotka sisältävät käyttöoikeuden määrittelyn, matkaviestinjärjestelmän 134 kotirekisteristä 130 kansainvälisen matkaviestintilaajan tunnuksen perusteella.

Eräässä suoritusmuodossa järjestelmä käsittää lisäksi laskutuspalvelimen 116, joka on konfiguroitu muodostamaan ensimmäisen tiedonsiirtoyhteyden 106 laskutustiedot, ja siirtämään laskutustiedot matkaviestinjärjestelmään 134, jossa laskutustiedot laskutetaan matkaviestinjärjestelmän 134 tilaajan tunnistetiedolle osoitetussa laskussa. Kuvion 1 esimerkissä meillä on tilanne, jossa tilaajapäätelaite 102 on vierailtavan matkaviestinjärjestelmän 126 alueella, jolloin laskutuspalvelimesta 116 siirretään laskutustiedot kotimatkaviestinjärjestelmän 134 laskutuspalvelimeen 132. Laskutustietojen siirto voidaan tehdä esimerkiksi IMSI:in kohdistettuja laskentatietueita (Charging Record, CDR) käyttäen.

Eräässä suoritusmuodossa palvelupiste 110 on konfiguroitu säilyttämään aluksi muodostettu tiedonsiirtolaitteen 100 ja palvelupisteen 110 väli-

nen ensimmäinen tiedonsiirtoyhteys 106 sisäänkirjautumiseen saakka. Tässä suoritusmuodossa ensimmäistä tiedonsiirtoyhteyttä 106 ei siis katkaista missään vaiheessa, jolloin pelkkä laittoman tunkeutujan suorittama salasanan kaappaaminen ei vielä aiheuta suurta tietoturvariskiä, sillä tunkeutujan täytyisi myös kyetä kaappaamaan ensimmäinen tiedonsiirtoyhteys 106. Tiedonsiirtoyhteys 106 käyttää esimerkiksi SSL-protokollaa (Secure Sockets Layer) TCP-yhteyksien (Transmission Control Protocol) autentikointiin ja salaamiseen. SSL:n sijasta voidaan käyttää myös protokollaa nimeltään TLS (Transport Layer Security). Käytettävät salausavaimet voidaan johtaa TLS-autentikoinnista tai vahvoilla salasana-autentikointiprotokollilla (esimerkiksi Secure Remote Password -protokolla tai Encrypted Key Exchange -protokolla) jopa pelkästä salasanasta lähtien.

Eräässä suoritusmuodossa autentikointipalvelin 114 on konfiguroitu lähettämään palvelupisteen 110 välityksellä toinen salasana tiedonsiirtolaitteelle 100 ensimmäistä tiedonsiirtoyhteyttä 106 käyttäen, ja tiedonsiirtolaite 100 on konfiguroitu käyttämään sisäänkirjautumisessa myös toista salasanaa, esimerkiksi siten, että kaksi salasanaa peräkkäin asetettuna muodostaa vaaditun salasanan. Tämä suoritusmuoto varmistaa, että toista salasanaa tarjoava käyttäjä on sama käyttäjä, joka tilasi salasanan tiedonsiirtolaitteella 100 tilaajapäätelaitteeseen 102.

Eräässä suoritusmuodossa autentikointipalvelin 114 on konfiguroitu lähettämään palvelupisteen 110 välityksellä varmennustunniste tiedonsiirtolaitteelle 100 ensimmäistä tiedonsiirtoyhteyttä 106 käyttäen, ja lähettämään salasanan lähetyksen yhteydessä tilaajapäätelaitteelle 102 sama varmennustunniste. Käyttäjä voi sitten verrata kahta, eri tiedonsiirtoteitä saamiansa varmennustunnisteita keskenään, ja käyttää salasanaa vain jos molemmat vastaanotetut varmennustunnisteet ovat samat. Tämä suoritusmuoto varmistaa käyttäjälle, että salasana tuli tilaajapäätelaitteeseen 102 samasta lähteestä 114, josta hän sitä pyysi tiedonsiirtolaitteellaan 100.

Eräässä suoritusmuodossa tiedonsiirtolaite 100 on konfiguroitu palvelupisteeseen 110 sisäänkirjauduttaessa käyttämään käyttäjätunnuksena matkaviestinjärjestelmän tilaajan tunnistetietoa, esimerkiksi jo aiemmin mainittua matkaviestintilaajan kansainvälistä ISDN-numeroa, tai sitten vaikkapa kansainvälistä matkaviestintilaajan tunnusta, joka voi tosin olla vaikeammin käyttäjän selville saatavissa kuin matkaviestintilaajan kansainvälinen ISDN-numero.

Tämän suoritusmuodon etuna on se, ettei järjestelmän tarvitse siirtää käyttäjätunnusta käyttäjälle päin.

Myös sellaiset suoritusmuodot ovat kuitenkin mahdollisia, joissa käyttäjätunnus siirretään järjestelmästä käyttäjälle päin. Tällöin käyttäjätunnuksen ei alunperin tarvitse olla käyttäjän tiedossa, vaan se voidaan generoida esimerkiksi autentikointipalvelimessa 114. Eräässä suoritusmuodossa autentikointipalvelin 114 on konfiguroitu lähettämään käyttäjätunnus matkaviestinjärjestelmän 134 tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen 102, ja tiedonsiirtolaite 100 on konfiguroitu palvelupisteeseen 110 sisäänkirjauduttaessa käyttämään käyttäjätunnuksena tilaajapäätelaitteeseen 102 toimitettua käyttäjätunnusta. Eräässä suoritusmuodossa autentikointipalvelin 114 on konfiguroitu lähettämään palvelupisteestä 110 käyttäjätunnus tiedonsiirtolaitteelle 100 ensimmäistä tiedonsiirtoyhteyttä 106 pitkin, ja tiedonsiirtolaite 100 on konfiguroitu palvelupisteeseen 110 sisäänkirjauduttaessa käyttämään käyttäjätunnuksena tiedonsiirtolaitteeseen 100 toimitettua käyttäjätunnusta.

Edellä on kuvattu miten palvelupistettä 110, autentikointipalvelinta 114, ja tiedonsiirtolaitetta 100 on konfiguroitava, jotta järjestelmä tiedonsiirtolaitteen 100 käyttäjän autentikointiin voidaan toteuttaa. Kyseiset laitteet sisältävät niiden toimintaa ohjaavia ohjausosia, jotka nykyisin toteutetaan yleensä prosessorina ohjelmistoineen, mutta myös erilaiset laitteistototeutukset ovat mahdollisia, esimerkiksi erillisistä logiikkakomponenteista rakennettu piiri tai yksi tai useampi asiakaskohtainen integroitu piiri (Application-Specific Integrated Circuit, ASIC). Myös näiden eri toteutustapojen sekamuoto on mahdollinen. Alan ammattilainen huomioi konfiguroinnin suorittavan toteutustavan valinnassa esimerkiksi laitteen koolle ja virrankulutukselle asetetut vaatimukset, tarvittavan prosessointitehon, valmistuskustannukset sekä tuotantomäärät.

Seuraavaksi kuvion 2 vuokaavioon viitaten selostetaan menetelmää tiedonsiirtolaitteen käyttäjän autentikointiin. Samalla viitataan kuvion 3 signaalisekvenssikaavioon, jolla havainnollistetaan tiedonsiirtolaitteen käyttäjän autentikoinnissa eri verkkoelementtien välillä lähetettävää informaatiota. Kuvion 3 selkiyttämiseksi palvelupiste 110 ja pääsykontrolleri 112 on yhdistetty yhdeksi elementiksi, eikä vierailtavan matkaviestinjärjestelmän 126 ja kotimatkaviestijärjestelmän 134 sisäisiä elementtejä kuvata.

Menetelmän suorittaminen aloitetaan 200:ssa käyttäjän halutessa käyttää palvelupistettä.

Aluksi 202:ssa muodostetaan tiedonsiirtolaitteella tiedonsiirtoyhteys palvelupisteeseen. Eräässä suoritusmuodossa tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys on radioyhteys. Eräässä suoritusmuodossa radioyhteys on toteutettu langattomalla lähiverkolla. Eräässä suoritusmuodossa radioyhteys on toteutettu lyhyen kantaman radiolähetinvastaanottimella. Eräässä suoritusmuodossa tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys on langallinen. Näiden tiedonsiirtoyhteyden eri toteuttamistapojen osalta viitataan aiempana olleeseen selostukseen.

Sitten 204:ssä syötetään 204 palvelupisteeseen matkaviestinjärjestelmän tilaajan tunnistetieto. Eräässä suoritusmuodossa matkaviestinjärjestelmän tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero. Kuvion 3 mukaisesti tiedonsiirtolaitteelta 100 lähetetään MSISDN 300 palvelupisteelle/pääsykontrollerille 110, 112.

Seuraavaksi 206:ssa tarkistetaan matkaviestinjärjestelmästä tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen. Eräässä suoritusmuodossa tarkistuksessa lähetetään kysely matkaviestinjärjestelmän kotirekisteriin. Suoritusmuodossa, jossa matkaviestinjärjestelmän tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero, voidaan kysely toteuttaa kuviossa 3 kuvattavalla tavalla siten, että kyselyssä selvitetään ensin matkaviestinjärjestelmän 134 kotirekisteristä matkaviestintilaajan kansainvälistä ISDN-numeroa vastaava kansainvälisen matkaviestintilaajan tunnus (IMSI) käyttäen MAP_SEND_IMSI-viestiä (MAP = matkapuhelinosaprotokolla, Mobile Application Part) 304, 306 ja siihen saatavaa REPLY:ä 308, 310, ja sitten selvitetään tilaajatiedot, jotka sisältävät käyttöoikeuden määrittelyn, matkaviestinjärjestelmän 134 kotirekisteristä kansainvälisen matkaviestintilaajan tunnuksen perusteella käyttäen MAP_RESTORE_DATA-viestiä 312, 314 ja siihen saatavaa REPLY:ä 316, 318. Koska kuvion 3 esimerkissä tilaajapäätelaite 102 on vierailtavan matkaviestinjärjestelmän 126 alueella, kulkevat viestit sen kautta kotimatkaviestinjärjestelmään 134 ja sieltä takaisin.

Sitten 208 tarkistetaan oliko matkaviestinjärjestelmän tilaajan tunnistetiedolla käyttöoikeus palvelupisteeseen. Jos käyttöoikeutta ei ole, tai se ei ole voimassa, niin siirrytään 210:een, jonka mukaisesti tiedonsiirtolaitteen käyttäjälle ei voida tarjota palvelua palvelupisteen kautta, jolloin siirrytään 220:een, jossa lopetetaan menetelmän suoritus.

Jos käyttöoikeus on voimassa, siirrytään 208:sta 212:een, jossa generoidaan salasana. Sitten siirrytään 214:ään, jossa lähetetään salasana mat-

kaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen. Eräässä suoritusmuodossa salasana lähetetään tilaajapäätelaitteeseen pakettikytkentäisenä viestinä. Eräässä suoritusmuodossa salasana lähetetään tilaajapäätelaitteeseen 102 lyhytsanomassa SMS 320, 322, 324, 326 kuviossa 3 kuvattavalla tavalla alkaen autentikointipalvelimesta 114, vierailtavan matkaviestinjärjestelmän 126, kotimatkaviestinjärjestelmän 134 ja lopuksi vielä vierailtavan matkaviestinjärjestelmän 126 kautta. Suoritusmuotoa voidaan muunnella aiemmin esitetyllä tavalla.

Seuraavaksi 216:ssa sisäänkirjaudutaan tiedonsiirtolaitteella palvelupisteeseen käyttäen salasanana tilaajapäätelaitteeseen toimitettua salasanaa. Kuviossa 3 tämä kuvataan sisäänkirjautumisdialogina, jossa käyttäjätunnus ja salasana lähetetään tiedonsiirtolaitteelta 100 palvelupisteeseen/pääsykontrolleriin 110, 112 LOGIN-viestissä 328, joka edelleen välitetään autentikointipalvelimeen 114 LOGIN-viestinä 330, johon tulee palvelupisteeseen/pääsykontrolleriin 110, 112 REPLY-viesti 332. Tämän jälkeen 218:ssa tiedonsiirtolaitteen käyttäjä voi käyttää palvelupisteen kautta tiedonsiirtopalveluita. Palvelu toteutetaan siirtämällä SERVICE-viestejä 334 molempiin suuntiin, tarpeen mukaan, tiedonsiirtolaitteen 100 ja palvelupisteen/pääsykontrollerin 110, 112 välillä. Lopuksi käyttäjän katkaistessa tiedonsiirtolaitteensa yhteyden palvelupisteeseen lopetetaan menetelmän suoritus 220:ssä.

Eräässä suoritusmuodossa menetelmä käsittää lisäksi: laskutetaan tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys matkaviestinjärjestelmän tilaajan tunnistetiedolle osoitetussa laskussa. Kuvion 3 mukaisesti tämä voidaan toteuttaa esimerkiksi siten, että palvelupisteestä/pääsykontrollerista 110, 112 siirretään laskutustietoa sisältävä CDR-viesti 336, 338 autentikointipalvelimen 114 kautta kotimatkaviestinjärjestelmään 134.

Eräässä suoritusmuodossa aluksi muodostettu tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys säilyy sisäänkirjautumiseen saakka. Tällä saavutetaan edellä kuvattu tietoturvaetu.

Eräässä suoritusmuodossa menetelmä käsittää lisäksi: lähetetään palvelupisteestä toinen salasana tiedonsiirtolaitteelle tiedonsiirtoyhteyttä käyttäen, ja sisäänkirjautumisessa käytetään myös toista salasanaa. Myös tämä suoritusmuoto parantaa edellä kuvatulla tavalla tietoturvaa.

Eräässä suoritusmuodossa menetelmä käsittää lisäksi: lähetetään palvelupisteestä varmennustunniste tiedonsiirtolaitteelle tiedonsiirtoyhteyttä käyttäen, ja salasanan lähetyksen yhteydessä tilaajapäätelaitteelle lähetetään

sama varmennustunniste, ja käytetään salasanaa vain jos molemmat vastaanotetut varmennustunnisteet ovat samat. Tämäkin suoritusmuoto kuvattiin jo aikaisemmin.

Eräässä suoritusmuodossa menetelmä käsittää lisäksi: käytetään sisäänkirjauduttaessa käyttäjätunnuksena matkaviestinjärjestelmän tilaajan tunnistetietoa. Eräässä suoritusmuodossa menetelmä käsittää lisäksi: lähetetään käyttäjätunnus matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen, ja käytetään sisäänkirjauduttaessa käyttäjätunnuksena lähetettyä käyttäjätunnusta. Eräässä suoritusmuodossa menetelmä käsittää lisäksi: lähetetään käyttäjätunnus tiedonsiirtolaitteelle tiedonsiirtoyhteyttä käyttäen, ja käytetään sisäänkirjauduttaessa käyttäjätunnuksena lähetettyä käyttäjätunnusta.

Menetelmän toteuttamiseen voidaan käyttää aikaisemmin kuvion 1 yhteydessä kuvattua järjestelmää, mutta muunkinlaiset ympäristöt voivat tulla kyseeseen.

Vaikka keksintöä on edellä selostettu viitaten oheisten piirustusten mukaiseen esimerkkiin, on selvää, ettei keksintö ole rajoittunut siihen, vaan sitä voidaan muunnella monin tavoin oheisten patenttivaatimusten esittämän keksinnöllisen ajatuksen puitteissa. Erityisesti on huomattava, että verkkoelementtien nimet ja toiminnallisuuksien jako voi vaihdella, lopultahan on vain kyse halutusta verkkoelementtien integrointiasteesta, ja myös tiedonsiirtoverkon 118 koosta: suurissa verkoissa verkkoelementti voi olla dedikoitu vain tietyille tehtäville, kun taas pienissä verkoissa yksi verkkoelementti voi hoitaa useita kuviossa 1 erillisiksi kuvattuja tehtäviä.

Patenttivaatimukset

1. Menetelmä tiedonsiirtolaitteen käyttäjän autentikointiin, joka menetelmä käsittää:

muodostetaan (202) tiedonsiirtolaitteella tiedonsiirtoyhteys palvelupisteeseen;

t u n n e t t u siitä, että menetelmä käsittää lisäksi:

syötetään (204) palvelupisteeseen matkaviestinjärjestelmän tilaajan tunnistetieto;

tarkistetaan (206) matkaviestinjärjestelmästä matkaviestinjärjestelmän tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen; ja

jos käyttöoikeus on voimassa, generoidaan (212) salasana, lähetetään (214) salasana matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen, ja sisäänkirjaudutaan (216) tiedonsiirtolaitteella palvelupisteeseen käyttäen salasanana tilaajapäätelaitteeseen toimitettua salasanaa.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että matkaviestinjärjestelmän tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero (MSISDN).

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tarkistuksessa lähetetään kysely matkaviestinjärjestelmän kotirekisteriin.

4. Patenttivaatimuksen 3 mukainen menetelmä, t u n n e t t u siitä, että matkaviestinjärjestelmän tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero, ja kyselyssä selvitetään ensin matkaviestinjärjestelmän kotirekisteristä matkaviestintilaajan kansainvälistä ISDN-numeroa vastaava kansainvälisen matkaviestintilaajan tunnus (IMSI), ja sitten selvitetään tilaajatiedot, jotka sisältävät käyttöoikeuden määrittelyn, matkaviestinjärjestelmän kotirekisteristä kansainvälisen matkaviestintilaajan tunnuksen perusteella.

5. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että salasana lähetetään tilaajapäätelaitteeseen pakettikytkentäisenä viestinä.

6. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että salasana lähetetään tilaajapäätelaitteeseen lyhytsanomassa.

7. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys on radioyhteys.

8. Patenttivaatimuksen 7 mukainen menetelmä, t u n n e t t u siitä, että radioyhteys on toteutettu langattomalla lähiverkolla.

9. Patenttivaatimuksen 7 mukainen menetelmä, t u n n e t t u siitä, että radioyhteys on toteutettu lyhyen kantaman radiolähetinvastaanottimella.

10. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys on langallinen.

11. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että menetelmä käsittää lisäksi: laskutetaan tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys matkaviestinjärjestelmän tilaajan tunnistetiedolle osoitetussa laskussa.

12. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että aluksi muodostettu tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys säilyy sisäänkirjautumiseen saakka.

13. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että menetelmä käsittää lisäksi: lähetetään palvelupisteestä toinen salasana tiedonsiirtolaitteelle tiedonsiirtoyhteyttä käyttäen, ja sisäänkirjautumisessa käytetään myös toista salasanaa.

14. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että menetelmä käsittää lisäksi: lähetetään palvelupisteestä varmennustunniste tiedonsiirtolaitteelle tiedonsiirtoyhteyttä käyttäen, ja salasanan lähetyksen yhteydessä tilaajapäätelaitteelle lähetetään sama varmennustunniste, ja käytetään salasanaa vain jos molemmat vastaanotetut varmennustunnisteet ovat samat.

15. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tiedonsiirtolaitteen ja palvelupisteen välinen tiedonsiirtoyhteys muodostetaan tilaajapäätelaitteen verkkovierailun aikana.

16. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että menetelmä käsittää lisäksi: käytetään sisäänkirjauduttaessa käyttäjätunnuksena matkaviestinjärjestelmän tilaajan tunnistetietoa.

17. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että menetelmä käsittää lisäksi: lähetetään käyttäjätunnus matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen, ja käytetään sisäänkirjauduttaessa käyttäjätunnuksena lähetettyä käyttäjätunnusta.

18. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että menetelmä käsittää lisäksi: lähetetään käyttäjätunnus tiedonsiirtolaitteelle tiedonsiirtoyhteyttä käyttäen, ja käytetään sisäänkirjauduttaessa käyttäjätunnuksena lähetettyä käyttäjätunnusta.

19. Järjestelmä tiedonsiirtolaitteen käyttäjän autentikointiin, joka järjestelmä käsittää tiedonsiirtolaitteen (100), tiedonsiirtolaitteeseen (100) ensimmäisellä tiedonsiirtoyhteydellä (102) kytkettävissä olevan palvelupisteen (110), ja palvelupisteeseen (110) toisen tiedonsiirtoyhteyden välityksellä kytketyn autentikointipalvelimen (114);

t u n n e t t u siitä, että:

palvelupiste (110) on konfiguroitu vastaanottamaan ensimmäistä tiedonsiirtoyhteyttä (106) pitkin tiedonsiirtolaitteella (100) syötetty matkaviestinjärjestelmän tilaajan tunnistetieto, ja lähettämään matkaviestinjärjestelmän tilaajan tunnistetieto toista tiedonsiirtoyhteyttä pitkin autentikointipalvelimelle (114);

autentikointipalvelin (114) on konfiguroitu tarkistamaan kolmatta tiedonsiirtoyhteyttä käyttäen matkaviestinjärjestelmästä (134) matkaviestinjärjestelmän tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen (110), ja jos käyttöoikeus on voimassa, generoimaan salasana ja lähettämään salasana matkaviestinjärjestelmän (134) tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen (102); ja

tiedonsiirtolaite (100) on konfiguroitu palvelupisteeseen (110) sisäänkirjauduttaessa käyttämään salasanana tilaajapäätelaitteeseen (102) toimitettua salasanaa.

20. Patenttivaatimuksen 19 mukainen järjestelmä, t u n n e t t u siitä, että matkaviestinjärjestelmän (134) tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero.

21. Patenttivaatimuksen 19 mukainen järjestelmä, t u n n e t t u siitä, että autentikointipalvelin (114) on AAA-palvelin (Authentication, Authorization, and Accounting).

22. Patenttivaatimuksen 19 mukainen järjestelmä, t u n n e t t u siitä, että autentikointipalvelin (114) on palvelupisteen (110) käyttöoikeuden tarkistamiseksi konfiguroitu lähettämään kysely matkaviestinjärjestelmän (134) kotirekisteriin (130).

23. Patenttivaatimuksen 22 mukainen järjestelmä, t u n n e t t u siitä, että matkaviestinjärjestelmän (134) tilaajan tunnistetieto on matkaviestintilaajan kansainvälinen ISDN-numero, ja autentikointipalvelin (114) on konfiguroitu kyselyssä ensin selvittämään matkaviestinjärjestelmän (134) kotirekisteristä (130) matkaviestintilaajan kansainvälistä ISDN-numeroa vastaavan kansainvälisen matkaviestintilaajan tunnuksen, ja sitten selvittämään tilaajatiedot,

jotka sisältävät käyttöoikeuden määrittelyn, matkaviestinjärjestelmän (134) kotirekisteristä (130) kansainvälisen matkaviestintilaajan tunnuksen perusteella.

24. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että autentikointipalvelin (114) on konfiguroitu lähettämään salasana tilaajapäätelaitteeseen (102) pakettikytkentäisenä viestinä.

25. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että autentikointipalvelin (114) on konfiguroitu lähettämään salasana tilaajapäätelaitteeseen (102) lyhytsanomassa.

26. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että ensimmäinen tiedonsiirtoyhteys (106) on radioyhteys.

27. Patenttivaatimuksen 26 mukainen järjestelmä, tunnettu siitä, että palvelupiste (110) on konfiguroitu toteuttamaan radioyhteys langattomalla lähiverkolla.

28. Patenttivaatimuksen 26 mukainen järjestelmä, tunnettu siitä, että palvelupiste (110) käsittää lyhyen kantaman radiolähetinvastaanottimen radioyhteyden toteuttamiseksi.

29. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että ensimmäinen tiedonsiirtoyhteys (106) on langallinen.

30. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että järjestelmä käsittää lisäksi laskutuspalvelimen (116), joka on konfiguroitu muodostamaan ensimmäisen tiedonsiirtoyhteyden (106) laskutustiedot, ja siirtämään laskutustiedot matkaviestinjärjestelmään (134), jossa laskutustiedot laskutetaan matkaviestinjärjestelmän (134) tilaajan tunnistetiedolle osoitetussa laskussa.

31. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että palvelupiste (110) on konfiguroitu säilyttämään aluksi muodostettu tiedonsiirtolaitteen (100) ja palvelupisteen (110) välinen ensimmäinen tiedonsiirtoyhteys (106) sisäänkirjautumiseen saakka.

32. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että autentikointipalvelin (114) on konfiguroitu lähettämään palvelupisteestä (110) toinen salasana tiedonsiirtolaitteelle (100) ensimmäistä tiedonsiirtoyhteyttä (106) käyttäen, ja tiedonsiirtolaite (100) on konfiguroitu käyttämään sisäänkirjautumisessa myös toista salasanaa.

33. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että autentikointipalvelin (114) on konfiguroitu lähettämään palvelupisteen (110) välityksellä varmennustunniste tiedonsiirtolaitteelle (100) ensimmäistä

tiedonsiirtoyhteyttä (106) käyttäen, ja lähettämään salasanan lähetyksen yhteydessä tilaajapäätelaitteelle (102) sama varmennustunniste.

34. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että ensimmäinen tiedonsiirtoyhteys (106) muodostetaan tilaajapäätelaitteen (102) verkkovierailun aikana.

35. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että tiedonsiirtolaite (100) on konfiguroitu palvelupisteeseen (110) sisäänkirjauduttaessa käyttämään käyttäjätunnuksena matkaviestinjärjestelmän tilaajan tunnistetietoa.

36. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että autentikointipalvelin (114) on konfiguroitu lähettämään käyttäjätunnus matkaviestinjärjestelmän (134) tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen (102), ja tiedonsiirtolaite (100) on konfiguroitu palvelupisteeseen (110) sisäänkirjauduttaessa käyttämään käyttäjätunnuksena tilaajapäätelaitteeseen (102) toimitettua käyttäjätunnusta.

37. Patenttivaatimuksen 19 mukainen järjestelmä, tunnettu siitä, että autentikointipalvelin (114) on konfiguroitu lähettämään palvelupisteen (110) välityksellä käyttäjätunnus tiedonsiirtolaitteelle (100) ensimmäistä tiedonsiirtoyhteyttä (106) pitkin, ja tiedonsiirtolaite (100) on konfiguroitu palvelupisteeseen (110) sisäänkirjauduttaessa käyttämään käyttäjätunnuksena tiedonsiirtolaitteeseen (100) toimitettua käyttäjätunnusta.

(57) Tiivistelmä

Keksinnön kohteena on menetelmä ja järjestelmä tiedonsiirtolaitteen (esimerkiksi langattoman lähiverkon, eli WLAN:in, päätelaite) käyttäjän autentikointiin. Menetelmässä muodostetaan (202) tiedonsiirtolaitteella tiedonsiirtoyhteys palvelupisteeseen. Sitten syötetään (204) palvelupisteeseen matkaviestinjärjestelmän tilaajan tunnistetieto (esimerkiksi MSISDN). Tämän jälkeen tarkistetaan (206) matkaviestinjärjestelmästä matkaviestinjärjestelmän tilaajan tunnistetiedon käyttöoikeus palvelupisteeseen. Jos käyttöoikeus on voimassa, generoidaan (212) salasana, lähetetään (214) salasana matkaviestinjärjestelmän tilaajan tunnistetietoa vastaavaan tilaajapäätelaitteeseen (esimerkiksi GSM-matkapuhelimeen), ja sisäänkirjaudutaan (216) tiedonsiirtolaitteella palvelupisteeseen käyttäen salasanana tilaajapäätelaitteeseen toimitettua salasanaa.

(Kuvio 2)

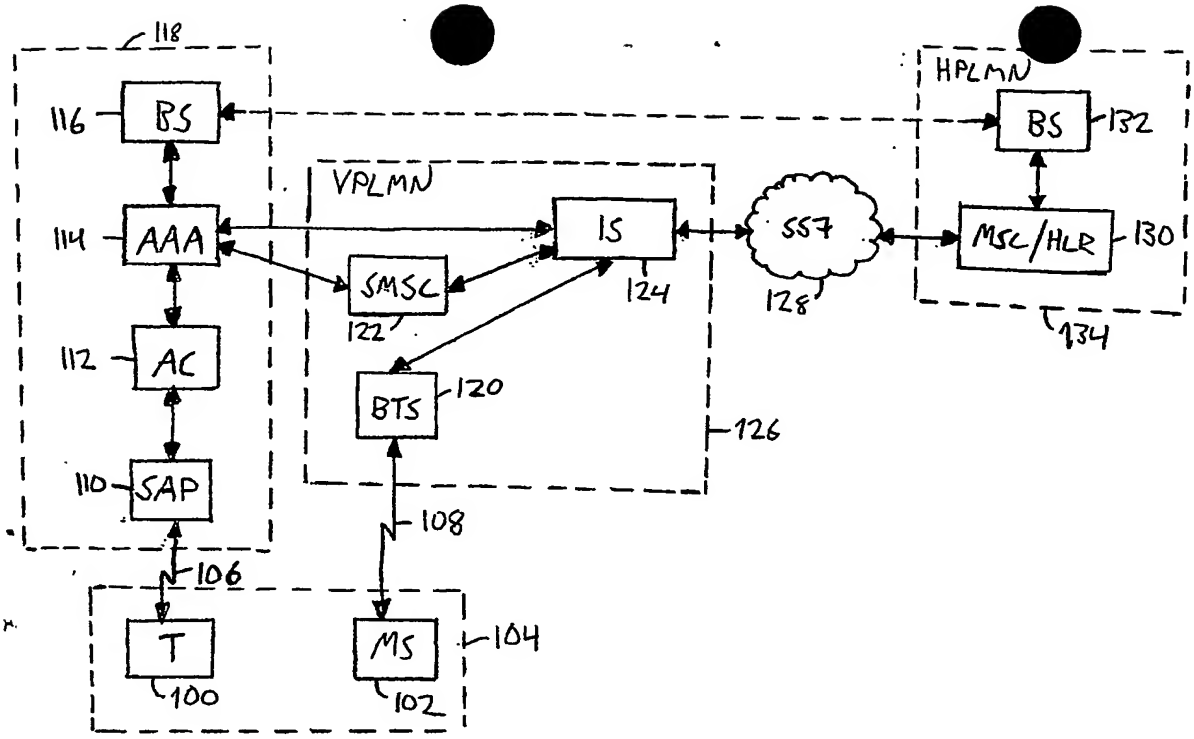
118
116
BS
114
AAA
112
AC
110
SAP
106
T
100
MS
102
104
VPLMN
IS
124
SMSC
122
BTS
120
126
108
557
128
HPLMN
BS
132
MSC/HLR
130
134

FIG. 1

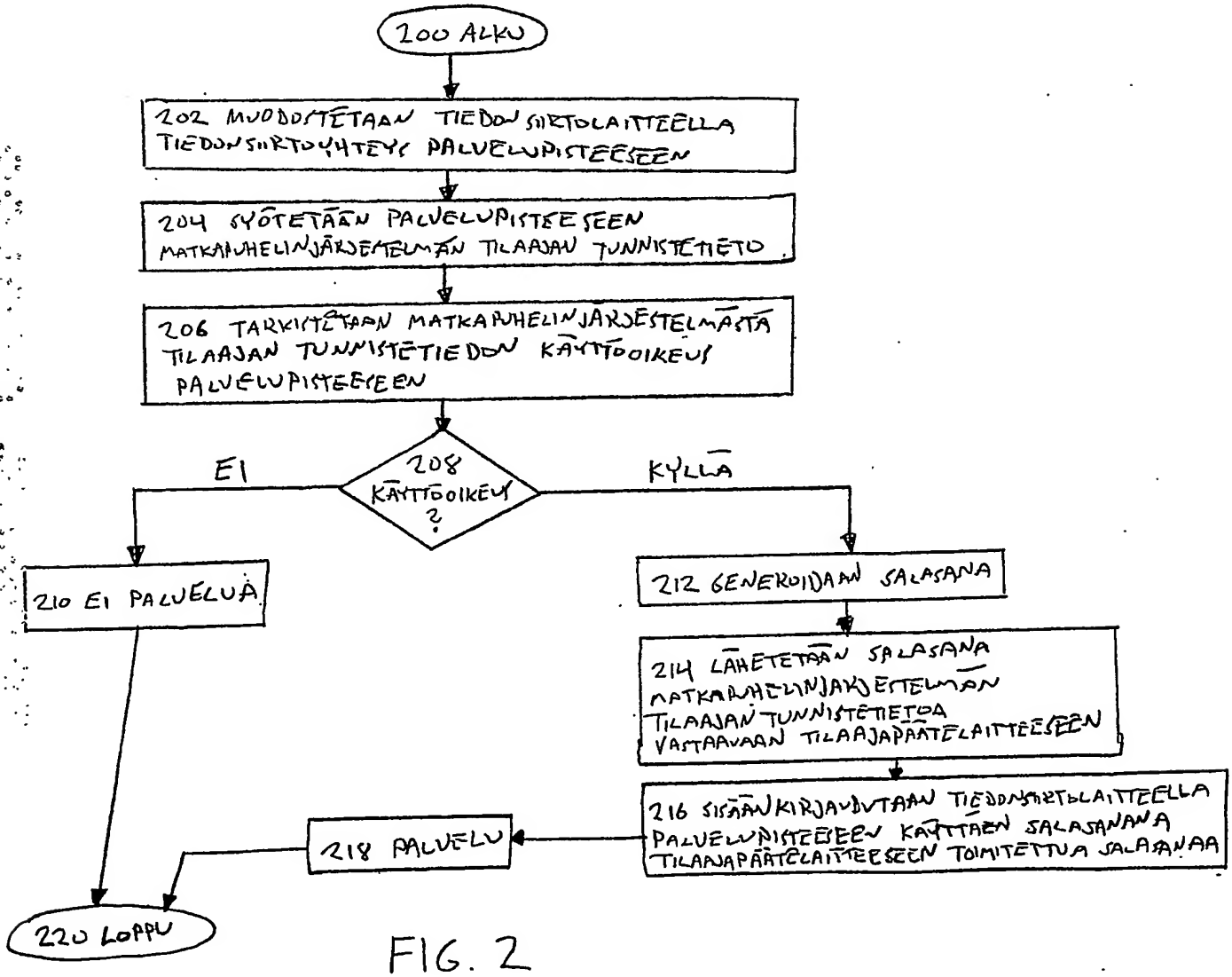
200 ALKU
202 MUODOSTETAAN TIEDONSIIRTOLAITTEELLA TIEDONSIIRTOYHTEYS PALVELUPISTEESEEN
204 SYÖTETÄÄN PALVELUPISTEESEEN MATKAPUHELINJÄRJESTELMÄN TILAAJAN TUNNISTETIETO
206 TARKISTETAAN MATKAPUHELINJÄRJESTELMÄSTÄ TILAAJAN TUNNISTETIEDON KÄYTTÖOIKEUS PALVELUPISTEESEEN
208 KÄYTTÖOIKEUS ?
EI
KYLLÄ
210 EI PALVELUA
212 GENEROIDAAN SALASANA
214 LÄHETETÄÄN SALASANA MATKAPUHELINJÄRJESTELMÄN TILAAJAN TUNNISTETIETOA VASTAAVAAN TILAAJAPÄÄTELAITTEESEEN
216 SISÄÄNKIRJAUDUTAAN TIEDONSIIRTOLAITTEELLA PALVELUPISTEESEEN KÄYTTÄEN SALASANANA TILAAJAPÄÄTELAITTEESEEN TOIMITETTUA SALASANAA
218 PALVELU
220 LOPPU

FIG. 2

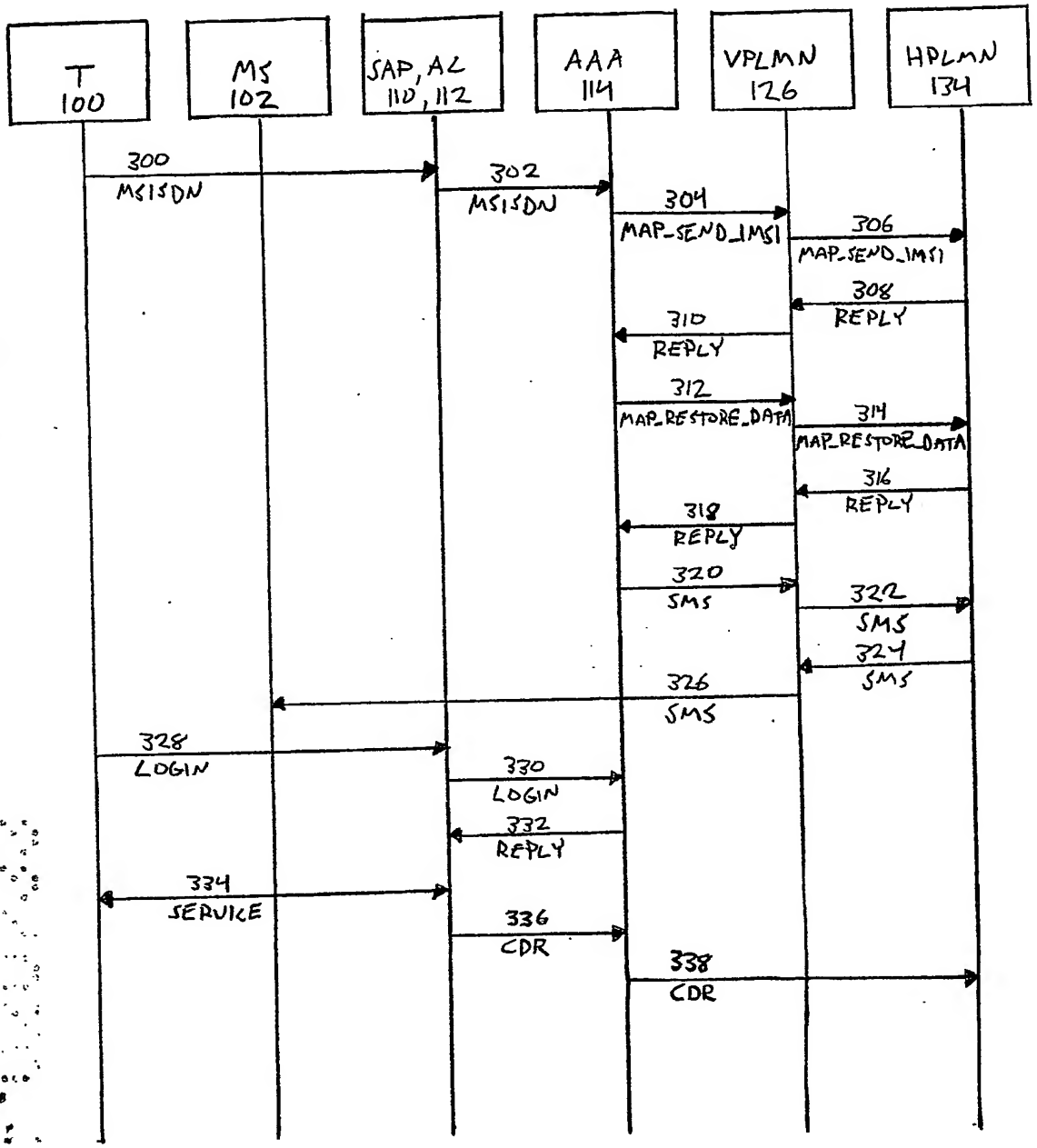
T
100
MS
102
SAP, AC
110, 112
AAA
114
VPLMN
126
HPLMN
134
300
MSISDN
302
MSISDN
304
MAP_SEND_IMSI
306
MAP_SEND_IMSI
308
REPLY
310
REPLY
312
MAP_RESTORE_DATA
314
MAP_RESTORE_DATA
316
REPLY
318
REPLY
320
SMS
322
SMS
324
SMS
326
SMS
328
LOGIN
330
LOGIN
332
REPLY
334
SERVICE
336
CDR
338
CDR

FIG. 3